Simon v. Adzilla, Inc [New Media] et al Doc. 292

Scott R. Mosko (State Bar No. 106070)
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.
Stanford Research Park
3300 Hillview Avenue
Palo Alto, California 94304
Telephone: (650) 849-6600
Facsimile: (650) 849-6666

Attorneys for Defendants
ConnectU LLC, Pacific Northwest
Software, Inc., Winston Williams, and
Wayne Chang

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

FACEBOOK, INC. and MARK ZUCKERBERG, Plaintiffs, v. CONNECTU LLC (now known as CONNECTU INC.), ET AL., Defendants.	CASE NO. C 07-01389 RS **DEFENDANTS CONNECTU LLC, PACIFIC NORTHWEST SOFTWARE, INC., WINSTON WILLIAMS, AND WAYNE CHANG'S OPPOSITION TO PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT** Date: February 27, 2008 Time: 9:30 a.m. Courtroom: 4 Judge: Honorable Richard Seeborg

REDACTED VERSION FOR PUBLIC VIEWING

Dockets.Justia.com

TABLE OF CONTENTS

		Page
I.	INTRODUCTION	1
II.	FACTS	1
III.	EVIDENCE OFFERED BY FACEBOOK IS INADMISSIBLE	3
IV.	SUMMARY JUDGMENT ON THE CAN-SPAM CLAIM IS INAPPROPRIATE	3
	A. Plaintiffs Were Not Adversely Affected by a Violation of the CAN-SPAM Act	4
	1. Plaintiffs' Alleged Harm Is Not Actionable Under CAN-SPAM	4
	2. Facebook Is Not An IASP	5
	3. Plaintiffs' Cannot Demonstrate Significant Harm	7
	B. Defendants' Alleged Emails Did Not Contain Materially False or Materially Misleading Header Information	9
	C. Defendants Did Not "Harvest" Email Addresses	11
	D. Defendants' Alleged Conduct Is Not an Aggravated Violation of CAN-SPAM	12
V.	SUMMARY JUDGMENT UNDER CALIFORNIA PENAL CODE § 502 IS INAPPROPRIATE	13
	A. California Penal Code § 502 Must Be Strictly Construed	13
	B. Defendants' Access Was Not "Unauthorized" or "Without Permission"	14
	C. Plaintiffs Offer No Evidence That They Are an "Owner or Lessee"	16
	D. Plaintiffs Suffered No "Damage or Loss" as a Result of Defendants' Actions	17
	1. "Victim Expenditure" Is Not Synonymous with "Damage or Loss"	17
	2. Additional Programming, If Any, Is Not Sufficient Damage or Loss	18
	E. The Data Obtained by ConnectU is not Private	21
VI.	PLAINTIFFS' UNCLEAN HANDS PRECLUDE SUMMARY JUDGMENT	22
	A. Zuckerberg's Attempts to Hack ConnectU's Servers Constitute Unclean Hands	22
	B. Unclean Hands Defense Creates a Genuine Issue of Material Fact	23
	C. Unclean Hands Is Available as a Defense to All of Plaintiffs' Claims	24

VII. UNDER FED. R. CIV. P. 56(f), SUMMARY JUDGMENT IS PREMATURE PENDING FURTHER DISCOVERY 25

VIII. CONCLUSION 26

TABLE OF AUTHORITIES

Page

FEDERAL CASES

Adler v. Federal Republic of Nig., 219 F.3d 869 (9th Cir. 2000) 9

Aitken v. Communications Workers of America, 496 F. Supp. 2d 653 (E.D. Va. 2007) 10

Ancata v. Prison Health Services, Inc., 769 F.2d 700 (11th Cir. 1985) 1

Bailey v. United States, 516 U.S. 137 (1996) 15

Buchanan Home & Automobile Supply Co. v. Firestone Tire & Rubber Co., 544 F. Supp. 242 (D.S.C. 1981) 10

Byron v. Clay, 867 F.2d 1049 (7th Cir. 1989) 10

Cabo Distributing Co. v. Brady, 821 F. Supp. 601 (N.D. Cal. 1992) 1, 6

Dollar System, Inc. v. Avcar Leasing System, Inc., 890 F.2d 165 (9th Cir. 1989) 9

Federal Commc'ns Commission v. America Broadcast Co., 347 U.S. 284 (1954) 13

Fuddruckers, Inc. v. Doc's B.R. Others, Inc., 826 F.2d 837 (9th Cir. 1987) 8

Haskell v. Time, Inc., 965 F. Supp. 1398 (E.D. Cal. 1997) 14

Hishon v. King & Spaulding, 467 U.S. 69 (1984) 1

In re Intuit Privacy Litigation, 138 F. Supp. 2d 1272 (C.D. Cal. 2001) 4

Kaap Industrial v. Burns & McDonnell Engineering Co., 2007 U.S. Dist. LEXIS 66064 9

L.A. News Serv. v. Tullo, 973 F.2d 791 (9th Cir. 1992) 9

Metropolitan Publishing v. San Jose Mercury News, 861 F. Supp. 870 (N.D. Cal. 1998) 9

Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348 (4th Cir. 2006) 9

Optinrealbig.com, LLC v. Ironport System, Inc., 323 F. Supp. 2d 1037 (N.D. Cal. 2004) 4

Platt v. Union Pac. R.R. Co., 99 U.S. 48 (1879) 15

Supermarket of Homes v. San Fernando Valley Board, 786 F.2d 1400 (9th Cir. 1986) 10

United States v. Middleton, 231 F.3d 1207 (9th Cir. 2000) 2-5

United States v. Sayklay, 542 F.2d 942 (5th Cir. 1976) 14

Wells Fargo & Co. v. Stagecoach Properties, Inc., 685 F.2d 302 (9th Cir. 1982) 8

STATE CASES

Blain v. Doctor's Co., 222 Cal. App. 3d 1048 (1990) 7

CrossTalk Products, Inc. v. Jacobson, 65 Cal. App. 4th 631 (1998) 7

DeRosa v. Transam. Title Insurance Co., 213 Cal. App. 3d 1390 (1989) 8

Fibreboard Paper Products v. E. Bay Union of Machinists, 227 Cal. App. 2d 675 9

Gordon v. Virtumundo, Inc., No. 06-0204-JCC, 2007 WL 1459395 (W.D. Wash. May 15, 2007) 4-8

Hill v. National Collegiate Athletic Ass'n, 7 Cal. 4th 1 (1990) 8

Hypertouch, Inc. v. Kennedy-W. University, No. C04-5203-SI, 2006 WL 648688 (N.D. Cal. Mar. 8, 2006) 5, 6, 8

Jacobs v. Universal Development Corp., 53 Cal. App. 4th 692 (1997) 9

Kendall-Jackson Winery v. Superior Court, 76 Cal. App. 4th 970 (1999) 7-8

Lass v. Eliassen, 94 Cal. App.175 (1928) 9

Mattco Forge v. Arthur Young & Co., 5 Cal. App. 4th 392 (1992) 9

Nader v. General Motors Corp., 255 N.E.2d 765 (1970) 9

Ossur Holdings, Inc. v. Bellacure, Inc., No. 05-1552, 2005 WL 3434440 (W.D. Wash. Dec. 14, 2005) 6

Timberline v. Jasinghani, 54 Cal. App. 4th 1361 (1997) 9

Unilogic Inc. v. Burroughs Corp., 10 Cal. App. 4th 612 (1992) 7-8

Wilson v. Harvey, 842 N.E.2d 83 (2005) 6

FEDERAL STATUTES

15 U.S.C. § 7701(a)(6) 4-5
15 U.S.C. § 7704(6) 9
15 U.S.C. § 7704(a)(1) 4, 9
15 U.S.C. § 7704(a)(1)(B) 10, 11
15 U.S.C. § 7704(a)(6) 9, 10
15 U.S.C.§ 7704(b) 11, 12
15 U.S.C. § 7704(b)(1)(A) 13
15 U.S.C. § 7704(b)(1)(B) 5
15 U.S.C. § 7706(g) 4, 6
15 U.S.C. § 7706(g)(3)(C) 12
15 U.S.C. § 7706(g)(3)(C)(i) 12
18 U.S.C. § 1030 4
18 U.S.C. § 1030(e)(8) 4
47 U.S.C. § 231(e)(4) 5
Fed. R. Civ. P. 56(f) 10
Fed. R. Civ. P. 30(b)(6) 10
Fed. R. Civ. P. 12(b)(6) 1, 10
Fed. R. Civ. P. 56(f) 10

STATE STATUTES

Cal. Penal Code § 502 .... 1, 14, 6
Cal. Penal Code § 502(a) 6, 14
Cal. Penal Code § 502(b)(9) 3
Cal. Penal Code § 502(c) 4

I. INTRODUCTION

Plaintiffs' motion relies upon uncorroborated and unauthenticated "evidence." It urges this Court to apply this "evidence" to statutory language, much of which has yet to be interpreted. In those circumstances when other courts have interpreted the statutes at issue, Plaintiffs' motion fails to even address these cases. Finally, this motion was filed before Defendants could complete discovery expected to show at least one of these statutes to be inapplicable.

The underlying facts concern ConnectU's permissive access onto Plantiffs' website. This authorization came from joint members of ConnectU's website and Facebook's website, who asked ConnectU to invite their friends listed on Facebook's website to join ConnectU. As explained in detail below, neither the CAN-SPAM statute nor Cal. Penal Code § 502 prohibits such activity.

Plaintiffs argue there are no issues of material fact, citing to the Court's decision on ConnectU's Motion to Dismiss. (Mot. at 15.) ConnectU disagrees, and will detail below several disputes of material fact. Moreover, Plaintiffs' reliance on the Order denying the Motion to Dismiss to support its summary judgment motion is entirely misplaced.[1] For the reasons set forth below, this motion must be denied.

II. FACTS

In late 2003/early 2004, Plaintiff Zuckerberg pirated ConnectU's Founders' idea for a social networking website and launched thefacebook.com (now facebook.com) before the Founders could launch their own website, connectu.com. After facebook.com launched, ConnectU's Founders wanted to visit facebook.com's site without having to join the site that pirated their idea, so they borrowed log-in information from friends and acquaintances. (*See* Mosko Decl., Ex. C, Winklevoss Dep. Trans. at p.25:17-25, 26: 1-25, 27: 1-25, 28:1.) Importantly, in every instance where ConnectU accessed a facebook.com page, it was at the behest and with the express permission from or through that friend. (Winklevoss Decl. ¶4.) Although certain email invitations to recipients with ".edu" email addresses were sent, none went to Facebook email accounts (i.e., [name]@facebook.com) and none of the emails were received or carried by Facebook's email servers. (Winklevoss Decl. ¶8.)

---

[1] In a motion to dismiss under Fed. R. Civ. P. 12(b)(6), the court must accept as true the pleaded facts and resolve them in the light most favorable to the plaintiff. *See Cabo Distrib. Co., Inc. v. Brady*, 821 F. Supp. 601, 608 (N.D. Cal. 1992) ("[T]he question presented by a motion to dismiss is not whether plaintiff will prevail in the action, but whether [the party] is entitled to offer evidence in support of [its] claim."). Thus, at the motion to dismiss stage, this Court was required to accept all of Facebook's factual allegations as true and view the factual allegations in a light most favorable to Facebook. *See Hishon v. King & Spaulding*, 467 U.S. 69, 73 (1984). Additionally, the threshold for Facebook's complaint to survive the motion to dismiss for failure to state a claim was "exceedingly low." *Ancata v. Prison Health Servs., Inc.*, 769 F.2d 700, 703 (11th Cir. 1985). In contrast, a court must apply an entirely different standard to summary judgment motions, where the court must view all of the evidence in a light most favorable to the non-movant. The court must look at all of the evidence produced during the discovery process and determine whether a genuine issue of material fact exists for trial. Findings made by this Court in the Order denying a motion to dismiss cannot, therefore, be relied on for summary judgment, as the relevant standards are entirely different.

To streamline this process, ConnectU developed a program called Importer/Social Butterfly. (Winklevoss Decl. ¶12; Williams Decl. ¶¶6, 7.) Through this program, after being asked by joint ConnectU/Facebook members to use their facebook.com logins and passwords to obtain email addresses from their Facebook profiles, ConnectU complied by using a program to find email addresses listed on the members' facebook.com profiles, rather than manually reviewing the profiles for the email addresses. (Winklevoss Decl. ¶12; Williams Decl. ¶7.) ConnectU then sent invitation emails to the ConnectU/Facebook members' friends who had requested that ConnectU login to their facebook.com accounts and invite their friends. (Winklevoss Decl. ¶15; Williams Decl. ¶¶9, 13.) The emails showed that they were from the members, and asked whether the friends wanted to join ConnectU. (Winklevoss Decl. ¶ 9.) ConnectU's Social Butterfly program also permitted ConnectU members who were also Facebook members to import their profiles from Facebook's website to the ConnectU website. (Winklevoss Decl. ¶13; Williams Decl.¶¶ 7, 8.) ConnectU only did this at the request of a ConnectU member. (Winklevoss Decl. ¶14; Williams Decl. ¶12.)

As the facebook.com site developed, friends' email addresses appeared as images. This change allowed the general public to access and see these email addresses by correctly typing the assigned URL into an Internet browser. (Williams Decl. ¶ 17.) There were no security measures on these public websites and access did not require an entry of a member's name or password. (Williams Decl. ¶ 17.) After this change was made, ConnectU accessed the friends' email addresses from the appropriate URLs without having to use the login information voluntarily provided from joint ConnectU/Facebook users. (Winklevoss Decl. ¶17; Williams Decl. ¶17.) Anyone with an Internet connection and a web browser could view the contents accessible by using these URLs. (Winklevoss Decl. ¶17; Williams Decl. ¶17.)

Plaintiffs contend this permission to access their site and later email invitations consistent with the wishes of joint Facebook/ConnectU members is actionable. However, significant questions of fact prevent the entry of summary judgment, including (1) whether ConnectU "hacked" into the facebook.com website. ConnectU's activities were conducted with permission and/or on public websites. (*see infra* Section IV.B); (2) whether Plaintiffs modified code or otherwise resecured facebook.com **in response** to ConnectU's actions (*see infra* Section V.D.2); (3) whether ConnectU sent any email to anyone containing materially false or materially misleading header information (*see infra* Section IV.B); (4) whether Plaintiffs were adversely affected by any conduct in violation of CAN-SPAM (*see infra* Section IV.A); (5) whether Defendants willfully or knowingly violated CAN-SPAM (*see infra* Section IV.D); (6) whether Defendants "harvested" email addresses through unauthorized automated means (*see infra* Section IV.C); (7) whether Plaintiffs are owners or lessees of facebook.com (*see infra* Section V.C); (8) whether Plaintiffs suffered "damage or loss" as a result of ConnectU's actions (*see infra* Section V.D); or (9) whether Zuckerberg's unclean hands precludes the relief sought by Plaintiffs (*see infra* Section VI).

In fact, most of these "questions of fact" should be answered in the negative. Indeed, Plaintiffs' servers never received a single email from Defendants, making it impossible for Plaintiffs to prove its claims (*see infra* Section V.A.). Plaintiffs' motion must be denied.

III. EVIDENCE OFFERED BY FACEBOOK IS INADMISSIBLE

Much of the evidence Plaintiffs use to support their Motion is inadmissible under the Federal Rules of Evidence and the Court cannot consider this evidence in ruling on this motion. Defendants refer the Court to their concurrently-filed Defendants' Objections to the Exhibits to the Declaration of Monte Cooper in Support of Plaintiffs' Motion for Partial Summary Judgment, incorporated herein by reference (hereinafter "Objections" and cited as "Objections to Ex. __").

IV. SUMMARY JUDGMENT ON THE CAN-SPAM CLAIM IS INAPPROPRIATE

To establish a private right of action under the CAN-SPAM Act (hereinafter "CAN-SPAM" or "the Act"), Plaintiffs must prove that Facebook is a provider of Internet access service and that it was adversely affected by a violation of §§ 7704(a)(1), 7704(b), or 7704(d)[2] of the Act, or a pattern or practice that violates § 7704(a)(2), (3), (4), or (5) of the Act.[3] *See* 15 U.S.C. § 7706(g); *Gordon v. Virtumundo, Inc.*, No. 06-0204, 2007 WL 1459395, at *2 (W.D. Wash. May 15, 2007). This Court must deny Plaintiffs' motion because there is a dispute of material fact (a) whether Plaintiffs have been adversely affected by Defendants' alleged conduct, and (b) whether any of the alleged emails sent by Defendants contained materially false or materially misleading header information.

A. Plaintiffs Were Not Adversely Affected by a Violation of the CAN-SPAM Act

Under 15 U.S.C. § 7706(g)(1), "A provider of Internet access service adversely affected by a violation of section 7704(a)(1) of this title . . . may bring a civil action . . . " To succeed in a private action under CAN-SPAM, Plaintiffs must show (1) that it was possible that they suffered harm recognized as actionable under CAN-SPAM; and (2) that the harm actually occurred. *Gordon*, 2007 WL 1459395, at *7. For the reasons set forth below, Plaintiffs fail to show that they were "adversely affected" by a violation of the CAN-SPAM Act, and cannot do so.

1. Plaintiffs' Alleged Harm Is Not Actionable Under CAN-SPAM

Plaintiffs' alleged "harm" or "loss" is not the type recognized by Congress in enacting CAN-SPAM, nor the type that an Internet service provider is entitled to remedy through CAN-SPAM's limited private right of action. *See* 15 U.S.C. § 7701(a)(6) ("The growth in unsolicited commercial electronic mail messages imposes significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions **that carry and receive such mail**, as there is a finite volume of mail that such providers, businesses, and institutions can handle without further investment in infrastructure.") (emphasis added); *see also Optinrealbig.com, LLC v. Ironport Sys., Inc.*, 323 F. Supp. 2d 1037, 1040 (N.D. Cal. 2004) (quoting CAN-SPAM Act, Pub. L. No. 108-

---

[2] 15 U.S.C. § 7704(a)(1) prohibits sending unsolicited commercial emails with materially false or misleading header information. Section 7704(b) deals with "aggravated violations," explained in more detail below, and § 7704(d) deals with warning label requirements for sexually oriented material, not at issue here.

[3] A pattern or practice claim must allege "deceptive subject headings" (§ 7704(a)(2)); "return address" and unsubscribe option violations (§ 7704(a)(3)); "transmission of commercial mail after objection" allegations (§ 7704(a)(4)); or "identifier, opt out, and physical address" violations (§ 7704(a)(5)). Plaintiffs do not argue violations of theses sub-sections, and provide no evidence of Defendants' alleged pattern or practice in violation of these subsections.

187 § 2(a)(6), (now codified at 15 U.S.C. § 7701(a)(6))). Because Plaintiffs' servers did not carry or transmit any of the alleged emails, Plaintiffs have not suffered any harm that can be remedied through CAN-SPAM. Rather, as stated by Plaintiffs repeatedly in their Motion (Mot. at 9, 11), the alleged emails were sent to Facebook's **users** at the users' email addresses issued by a college or university, via the school's server.[4] (Winklevoss Decl. ¶¶ 7, 8) Plaintiffs have not and could not allege that **Facebook's** servers received a single email sent by Defendants. Thus, Plaintiffs cannot possibly allege *any* harm or loss as a result of any conduct in violation of the CAN-SPAM Act. *See Gordon*, 2007 WL 1459395, at *7 ("These harms to IASs [Internet access services] or ISPs [Internet service providers] relate to network functioning, bandwidth usage, increased demands for personnel, and new equipment needs, which eventually cost consumers.")

2. Facebook Is Not An IASP

Facebook lacks standing to bring suit under the Act because it is not a provider of Internet access service ("IASP").[5] While this Court has held that an Internet company that provided its own email servers, and nothing else, had standing as a provider of Internet access service, there is at least a question of fact regarding Plaintiffs' standing in this case. *Hypertouch, Inc. v. Kennedy-Western University*, U.S. Dist. No. C 04-05203, 2006 WL 648688, at *3 (N.D. Cal. March 8, 2006). In finding that the plaintiff there had standing, this court analyzed the Congressional justifications for the Act and found that one of the concerns of Congress was the cost that Internet service providers must bear in responding "to rising volumes of spam by investing in new equipment to increase capacity." *Id.*, *citing* Report of the Committee on Commerce, Science, and Transportation on S. 877, S. Rep. No. 102, 108th Cong., 1st Sess. 6 (2003). The Court emphasized that the plaintiff "administers its own e-mail servers, and is therefore the entity that is potentially forced to increase its capacity due to spam sent to e-mail addresses hosted by those servers." *Id.* Here, on the other hand, Facebook would not be subject to any of the harm recognized by this Court. Facebook does not provide its users with email accounts or addresses. Thus, it would not be burdened with increasing the capacity of its servers in response to unsolicited emails.

---

[4] Simply because Facebook's users voluntarily placed email addresses on their Facebook profiles does not give Plaintiffs a legal or proprietary interest in the email addresses. In its discussion of aggravated violations of CAN-SPAM, Congress made clear that the Act does not "create[] an ownership or proprietary interest in such electronic mail addresses." 15 U.S.C. § 7704(b)(1)(B).

[5] The Act defines Internet access service as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services." 47 U.S.C. § 231(e)(4) (2006).

In its ruling on a motion to dismiss, this Court denied Defendants' argument that Facebook[6] did not have standing because it was not an IASP under the Act. (Dkt. 73.) But this ruling can only be interpreted to mean that Facebook's pleading included sufficient allegations that it **might** qualify as an IASP. *See Cabo Distrib.*, 821 F. Supp. at 608 ("[T]he question presented by a motion to dismiss is not whether plaintiff will prevail in the action, but whether [the party] is entitled to offer evidence in support of [its] claim."). In Plaintiffs' motion, however, there is no admissible evidence allowing the Court to make such a finding, and given the admissible evidence regarding the characteristics of Facebook as compared to the requirements for an IASP, there is a dispute of material fact as to whether Facebook is an IASP. Moreover, evidence that Facebook is not an IASP under the Act is the **exact** evidence that Defendants had hoped to obtain based on their 30(b)(6) deposition of Facebook pursuant to Rule 56(f). As explained below, Section VII, *infra*, Plaintiffs did not offer to make a witness available until **after** Defendants opposition to this motion was due.

Even if the Court concludes that Facebook is an IASP under CAN-SPAM, to prevail under CAN-SPAM, Facebook's "adverse effect" must have been "both real and the type uniquely experienced by IASs for standing to exist." *Gordon*, 2007 WL 1459395, at *7 ("Any other reading would expand the private right of action beyond what Congress intended."). This Court has recognized that adverse effect under the Act includes "decreased server response and crashes . . . higher bandwidth utilization, and forced expensive hardware and software upgrades." *Hypertouch*, 2006 WL 648688, at *4. **None** of these elements are alleged.[7] Nor do Plaintiffs submit any evidence of these elements. Accordingly, at the **very least**, there is a disputed material fact as to an essential element of Plaintiffs' private right of action under CAN-SPAM—namely, whether it was even possible for Facebook to be "adversely affected" under the Act.

---

[6] Facebook added Zuckerberg as a Plaintiff in its Second Amended Complaint, served after this Court ruled on ConnectU's Motion to Dismiss. (Dkt. 75) Clearly, Zuckerberg, an individual, does not have standing to bring a private right of action under CAN-SPAM, as an IASP. *See* 15 U.S.C. § 7706(g).

[7] In support of their claim of adverse effect, Plaintiffs cite the legislative history of the Act (*See* Mot. at 24-25), which states only that an IASP whose email addresses were "harvested" **could** be adversely affected. There is an initial question of fact as to what "harvest" means. Defendants assert they did not "harvest" email addresses. Rather, they used the email addresses of a Connect/Facebook members' friends, at

(continued...)

3. Plaintiffs' Cannot Demonstrate Significant Harm

Even if it were **possible** for Plaintiffs to have been adversely affected by any of Defendants' alleged conduct in violation of CAN-SPAM, the Plaintiffs' alleged "harm" and "loss" fall miles short of the significant adverse effect required for a private action under CAN-SPAM. *See Gordon*, 2007 WL 1459395, at *8 ("Not only must CANSPAM private plaintiffs allege a particular type of harm, the adverse effect they allege must be significant.") Plaintiffs seek millions of dollars in statutory damages under CAN-SPAM, but do not request actual damages under the Act. As the *Gordon* court observed, "permitting private parties with **no harm** to invoke CAN-SPAM to collect millions of dollars surely is not what Congress intended when it crafted this 'limited' private right of action." The *Gordon* court also said "[t]he necessity of a showing of significant adverse effect is particularly evident in the instant case, where Plaintiffs seek **solely** statutory damages [amounting to nearly $2.5 million]." *Id.* At the very least, a question of fact exists as to whether Plaintiffs suffered a **significant** adverse effect.

Indeed, the only "harm" or "loss" Plaintiffs allege is an unsubstantiated belief that they lost advertising money due to the [redacted] of their members as a result of allegedly receiving emails from Defendants,[8] and Plaintiffs' alleged modification of the Facebook code to "stop Defendants' efforts to acquire data from Facebook's site."[9]

(...continued)
the members' request. Second, even if Facebook could be adversely affected, it has not demonstrated that it actually was adversely affected, and at the very least there is a dispute of material fact as to any adverse effect.

[8] *See* Mosko Decl., Ex. A, Zuckerberg Dep. Transcript at 243:17-25; 242:7-18) ("But ConnectU in making this program basically made something that was going to go through and find e-mail addresses and spammed all these people. So not only did that effect[sic] our users negatively but it decreased their trust in us.")

[9] Specifically, Plaintiffs allege that they (1) modified the Facebook code to block the Social Butterfly program;(2) sought to prevent Defendants from copying email addresses with javascript, and by rendering email addresses as images; (3) wrote code to identify and block Links and Lynx; (4) created the 'Karma' script to prevent automated system attacks; and (5) Zuckerberg and Moskovitz spent 3-4 days producing new code to counteract Defendants' efforts. (Mot. at p. 12-14)

[redacted] is not an adverse effect actionable under CAN-SPAM. Even if [redacted] were an adverse effect recognized by CAN-SPAM, Plaintiffs have no evidence to support their contention that users lost trust in Facebook. (*See* Mosko Decl., Ex. A, Zuckerberg Dep. Tr. at 244: 2-13; 246: 7-9) [redacted] When specifically asked how Plaintiffs had been harmed, Zuckerberg responded that [redacted] (*Id.* at 251: 6-22.) When specifically asked if Plaintiffs were aware of the loss of any specific users, Zuckerberg responded: [redacted] (*Id.* at 252: 1-4; 254: 1-7)

In addition, Zuckerberg's "modification" of the Facebook code certainly does not amount to the "forced expensive hardware and software upgrades" that this Court has recognized as an adverse effect under CAN-SPAM. *Hypertouch*, 2006 WL 648688, at *4.

With respect to Plaintiffs' code modifications, much of that alleged "harm" is supposedly supported by the declaration of Plaintiffs' expert, Chris Shiflett. (*See* Mot. at 12-14.) But the Shiflett Declaration does not claim that any such "harm" was incurred in direct response to any of Defendants' alleged conduct. (Williams Decl. ¶21.) Mr. Shiflett is not a fact witness so his suggestion that "harm" resulted from Defendants' acts is irrelevant. Indeed, the code Shiflett analyzed shows that all of Plaintiffs' "efforts" were routine procedures that any large-volume website would utilize. Because none of the "harm" alleged in the Shiflett Declaration was in response to Defendants' alleged conduct, the Declaration does not provide any evidence that any harm actually occurred as a result of Defendants' conduct. *See Gordon*, 2007 WL 1459395, at *7 ("[I]t follows that [harm under CAN-SPAM] must be (1) possible and (2) actually occur.").

Thus, whether Plaintiffs have demonstrated the significant adverse effect required by a limited private right of action under CAN-SPAM is a disputed material fact. In view of the foregoing disputed issues, Plaintiffs' motion should be denied with respect to CAN-SPAM.

B. Defendants' Alleged Emails Did Not Contain Materially False or Materially Misleading Header Information

Plaintiffs allege that ConnectU and Pacific Northwest Software, Inc. ("PNS") violated § 7704(a)(1) of the CAN-SPAM Act. (Mot. at 19.) This provision makes unlawful the initiation of a commercial email message that contains, or is accompanied by, "header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). Plaintiffs cannot demonstrate that any of the alleged emails sent by the Defendants contained materially false or materially misleading header information, and whether any header information was materially false or misleading is a disputed material fact. Indeed, Plaintiffs implicitly concede that there is no evidence that the alleged emails contained materially false or misleading headers because while they repeatedly argue that the emails contained "false" or "misleading" header information, they **never** contend that the information was **materially** misleading or false, as is required for a claim under § 7704(a)(1).[10] *See id.*

The present facts are analogous to *Omega World Travel, Inc. v. Mummagraphics, Inc.*, 469 F.3d 348, 357-58 (4th Cir. 2006) (holding that defendant was entitled to summary judgment on CAN-SPAM claims because plaintiff did not show that inaccurate headings were materially misleading). Here, as in *Omega*, any emails allegedly sent by the Defendants were "chock full of methods to 'identify, locate, or respond to' the sender." *Id.* at 357 (quoting 15 U.S.C. § 7704(a)(6)). Here, as in *Omega*, the emails allegedly sent by the Defendants were "replete with accurate identifiers of the sender" such that the alleged inaccuracies in the headers could not have impaired the efforts of any recipient to identify the sender. *Id.* at 358. All of the emails cited by Plaintiffs in their motion include a hyperlink to http://www.connectu.com. (*See* Winklevoss Decl. ¶11; Williams Decl. ¶16) Moreover, the emails are replete with references to ConnectU. (*Id.*) Finally, as Plaintiffs explain in their motion, recipients could respond to the email and send a message to webmaster@connectu.com, and thereby ask not to receive additional emails. (Mot. at 10) This evidence creates another dispute of material fact as to whether any of the alleged emails contained **materially** false or misleading header information.

---

[10] The Act defines "materially" as "the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of the recipient of the message to respond to a person who initiated the electronic message." 15 U.S.C. § 7704(6).

Plaintiffs vainly attempt to analogize the facts in this case to the facts in *Aitken v. Commc'ns Workers of Am.*, 496 F. Supp. 2d 653 (E.D. Va. 2007). (Mot. at 21-22) However, *Aitken* is distinguishable for a number of reasons. First, the *Aitken* court ruled on a motion to dismiss under Fed. R. Civ. P. 12(b)(6). *Id.* at 656. The court noted that it was considering the plaintiff's claims at the "threshold stage" and drew "reasonable inferences . . . in plaintiff's favor." *Id.* at 667 n.12. Here, Plaintiffs are moving for summary judgment and are required to demonstrate that the alleged emails undisputedly contained materially false or misleading header information. Accordingly, the *Aitken* court's holding that the plaintiff alleged sufficient facts to state a claim under § 7704(a)(1) is irrelevant here.

Second, the *Aitken* court ruled that, at the pleading stage, header information was materially false or misleading because the defendants created false sender email addresses using the names of the plaintiff's managers without the permission of those managers. *Id.* at 657. Here, on the other hand, the email addresses were obtained with permission of the ConnectU/Facebook members, with the understanding that ConnectU would send email messages to all of the members' friends. (Winklevoss Decl. ¶¶4, 9, 14, 15; Williams Decl. ¶¶10, 13.) Thus, there is no concern, as there was in *Aitken*, that a recipient might incorrectly judge "the value" of the incoming message because it would not be incorrect to assume that the message was sent at the behest of the member. Here, the Facebook/ConnectU member whose name appeared in an email expressly authorized ConnectU to send an invitation email to his/her friends on his/her behalf. (Winklevoss Decl. ¶15; Williams Decl. ¶¶10, 13.) Thus, a heading showing that the email came from the member was not materially false or misleading, but in fact was accurate and easily understood. *See* 15 U.S.C. § 7704(a)(1)(B) ("[A] from line (the line identifying or purporting to identify a person initiating the message) that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading.").

Plaintiffs also allege that the Defendants sent emails from "fabricated addresses." (*Id.* at. 22.) Again, Plaintiffs fail to allege that any of the header information for these emails was **materially** false or misleading — nor could Plaintiffs do so. Moreover, the evidence Plaintiffs cite in support of this allegation is inadmissible hearsay, lacks foundation, and is unauthenticated. (*See* Objections to Ex. 26 and 29.) Because Plaintiffs have provided no evidence supporting an essential element of their claim, i.e., materiality of the alleged false header information, Plaintiffs have not satisfied their burden, and thus there is a dispute of material fact as to whether any of the alleged "fabricated addresses" contained materially false or misleading header information.

C. Defendants Did Not "Harvest" Email Addresses

Plaintiffs waste a lot of paper arguing that Defendants "harvested" email addresses. First, Defendants did not harvest email addresses. Rather, in all instances when Defendants accessed Facebook members' accounts via Social Butterfly, it was at the behest of the ConnectU/Facebook member, and with the express permission of the ConnectU/Facebook member to use his or her friends' email addresses to send invitation emails. (Winklevoss Decl. ¶¶14, 15; Williams Decl. ¶¶12, 13.) Second, email address "harvesting" is not, in and of itself, a violation of the Act. *See* 15 U.S.C. § 7704(b). Rather, the Act only makes email-address harvesting actionable if the email addresses that were allegedly harvested were **actually used** to send unsolicited commercial emails in violation of § 7704(a) of the Act. *Id.* Not only have Plaintiffs failed to provide any admissible evidence that any of the alleged emails sent by Defendants contained materially misleading headers, or violated any other provision of § 7704(a), but Plaintiffs have failed to put forth any evidence showing that the emails they claim contained materially misleading headers were sent to email addresses that were allegedly "harvested" from Facebook's website. At the very least, this creates a dispute of material fact as to whether Defendants "harvested" emails in any manner prohibited by the Act.

D. Defendants' Alleged Conduct Is Not an Aggravated Violation of CAN-SPAM

In addition to the factual issues detailed above, there is a genuine issue of material fact as to whether Plaintiffs are entitled to aggravated damages under § 7706(g)(3)(C).[11] As explained above, Plaintiffs cannot demonstrate that any alleged email sent by the Defendants contained materially false or misleading header information in violation of § 7704(a)(1), and cannot demonstrate that they have been adversely affected as that term is used in the Act. Because Plaintiffs are not entitled to any damages, they certainly cannot be entitled to aggravated damages. In any event, there are genuine issues of material fact regarding Plaintiffs' claim of aggravated damages.

Plaintiffs have not submitted competent evidence that the Defendants' alleged behavior was willful and knowing. *See* 15 U.S.C. § 7706(g)(3)(C)(i). Plaintiffs' evidence that purports to show that ConnectU had actual knowledge that its conduct violated the Act is not competent and does not demonstrate that ConnectU had any such knowledge. First, the email from Northeastern University is hearsay and lacks foundation. (*See* Objections to Ex. 29.) Second, a nonparty information technology security manager's interpretation of the legalities of emails does not demonstrate that Cameron Winklevoss, or anyone at ConnectU, had knowledge or the belief that they were violating the Act. (*See* Objections to Ex. 45.) Third, the fact that a person at iMarc may have told ConnectU that it should be "worried" does not show that ConnectU had knowledge or the belief that its conduct violated the Act. (*See* Objections to Ex. 29.) To the contrary, as explained in his declaration, Cameron Winklevoss was not aware that Facebook or Zuckerberg were asserting that ConnectU's conduct violated the Act until Facebook filed this action. (Winklevoss Decl. ¶ 18.) Indeed, a CAN-SPAM claim was not even alleged until a year after this case commenced. Whether ConnectU knowingly and willfully violated the Act is therefore a dispute of material fact, precluding summary judgment.

Similarly, none of the evidence presented by Plaintiffs in their motion demonstrates that PNS violated the Act willfully and knowingly. (*See* Mot. at 22-23.) First, Chang's statement in his email that "Facebook is starting to catch on" in no way indicates that any of the Defendants knowingly and willfully violated the Act. (*See* Objections to Ex. 45.) Moreover, Chang's use of "illegally" refers to the use of logins and passwords to log into other networks and makes no reference to the sending of any emails. (*See* Objections to Ex. 34.) Even if this evidence did support Plaintiffs' claim that PNS willfully violated the Act, it is inadmissible because it lacks foundation and it is unauthenticated. (*See* Objections to Exs. 29, 34, 45.) Whether PNS knowingly and willfully violated the Act is therefore a dispute of material fact, precluding summary judgment.

---

[11] The Act permits aggravated damages if a court determines that (i) the defendant committed the violation willfully and knowingly; or (ii) the defendant's violation included one or more of the aggravated violations set forth in 15 U.S.C. § 7704(b). 15 U.S.C. § 7706(g)(3)(C).

Finally, there is a genuine issue of material fact as to whether Defendants' activities violated § 7704(b)(1)(A)(i).[12] The evidence relied upon by Plaintiffs to support their argument that the Defendants' conduct was an aggravated violation under § 7704(b) is based on an instant-message conversation obtained from David Gucwa. (*See, e.g.*, Mot. at 6-9.) There is **no authentication** for any of the statements in the instant-message conversation, and Plaintiffs' counsel's declaration that it is a true and correct copy is insufficient. (*See* Objections to Ex. 9.) In any event, as explained above, Plaintiffs failed to offer evidence demonstrating that any of the alleged emails violated § 7704(a), and absent such evidence, Plaintiffs cannot demonstrate that the Defendants violated § 7704(b)(1). *See* 15 U.S.C. § 7704(b)(1)(A) (requiring a violation of § 7704(a) as a prerequisite for an aggravated violation under § 7704(b)(1)). Accordingly, there is a genuine issue of material fact regarding Defendants' alleged aggravated violations of § 7704(b)(1).

V. SUMMARY JUDGMENT UNDER CALIFORNIA PENAL CODE § 502 IS INAPPROPRIATE

A. California Penal Code § 502 Must Be Strictly Construed

Because California Penal Code § 502 is part of the penal, rather than civil code, it must be strictly construed. *See Fed. Commc'ns Comm'n v. Am. Broad. Co.*, 347 U.S. 284, 296 (1954) (a statute with provisions for both criminal and civil liability must be strictly construed); *accord*

[12] Section 7704(b)(1)(A)(i) makes an aggravated violation of the Act the transmission of an email in violation of any of the provisions of § 7704(a), coupled with the sender's knowledge that the recipient's email address was "obtained using automated means from an Internet website or proprietary online service." 15 U.S.C. § 7704(b)(1)(A)(i).

Haskell v. Time, Inc., 965 F. Supp 1398, 1404 (E.D. Cal. 1997). When interpreting criminal statutes, even in the context of civil litigation, a court must strictly construe the terms used in the criminal statute at issue. *Id.* Each word must be narrowly interpreted and may not be enlarged by implication or intent, and cannot be held to encompass offenses and individuals other than those clearly described and provided for in the statutory language. Any ambiguity in a criminal statute must be resolved in favor of the defendant. *U.S. v. Sayklay*, 542 F.2d 942, 944 (5th Cir. 1976) (holding that penal statutes are strictly construed with ambiguities resolved in favor of the defendant) (citing *U.S. v. Enmons*, 410 U.S. 396, 411 (1973)).

Plaintiffs' motion requires the Court to evaluate the meanings of several terms used in §§ 502(a), 502(c)(2), 502(c)(6), 502(c)(7), and 502(e),[13] the definitions of which are issues of first impression, and determine whether Defendants' actions are encompassed by those definitions. Applying the rules of strict construction, the Court cannot find, as a matter of law, that Defendants violated § 502 because the definitions of material terms, and their application to the claim, constitute disputes of material fact not appropriate for decision on summary judgment.

To prevail on summary judgment, Plaintiffs must establish each element of a § 502 violation. Moreover, and of equal importance, Plaintiffs must show that there are no disputes of material fact regarding any element of the claim. Plaintiffs have not, and cannot, do so. Indeed, in their Motion, Plaintiffs failed to identify and address each component element of a § 502 violation. As detailed below, there are several disputes of material fact stemming from the language of § 502 that preclude summary judgment.

B. Defendants' Access Was Not "Unauthorized" or "Without Permission"

Section 502(a) of the statute explicitly states that the purpose of the statute is to protect "individuals, businesses, and governmental agencies from tampering, interference, damage, and **unauthorized** access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a) (emphasis added).[14] Sections 502(c)(2), 502(c)(6), and 502(c)(7) require that the alleged

---

[13] These are the sections of Cal. Penal Code § 502 asserted by Plaintiffs. (Mot. at 15-19.)

[14] Facebook does not argue that ConnectU tampered with, interfered with, or damaged its computer system.

"access" be "**without permission**." (Emphasis added.) The statute makes no effort to define or distinguish the terms "unauthorized" and "without permission." While in common parlance these terms may be synonymous, it is axiomatic that each word of a statute must have meaning, and that no term is extraneous. *Platt v. Union Pac. R.R. Co.*, 99 U.S. 48, 58 (1879) ("[T]he admitted rules of statutory construction declare that a legislature is presumed to have used no superfluous words."). Because this is a case of first impression, it falls to this Court not only to define these terms within the confines of strict construction, but also to distinguish their meanings. *Bailey v. U.S.*, 516 U.S. 137, 146 (1995) ("We assume that Congress used two terms because it intended each term to have a particular, non superfluous meaning."). This ambiguity alone should be sufficient to overcome summary judgment, as there is a genuine issue of material fact as to who may grant "authorization" or "permission" under the statute.

Relying on facebook.com's Terms of Use, Plaintiffs claim that it is an undisputed fact that Defendants' access was "unauthorized" and/or "without permission." (Mot. at 18.) Defendants vigorously dispute that their access to the Facebook website was "unauthorized" or "without permission." Rather, as explained in Section II, *supra*, Defendants accessed the Facebook website with the permission of Facebook members, who had provided to Defendants their login identification. When using a friend's login information, ConnectU entered only the portions of the Facebook website that would have been available to that member had he personally logged in, *i.e.*, the member's own profile page. (Winklevoss Decl. at ¶ 5.) Defendants never attempted to view or otherwise access any information on the Facebook website that was not available to either the Facebook member whose login information was being used, or to the public at large. (*Id.*) Cognizant of the potential issues associated with obtaining information by circumventing any security mechanisms, such as firewalls, in the Facebook website, Defendants deliberately devised procedures that they believed were within the rules because they intentionally did **not** bypass any such security system. (*Id.*)

ConnectU/Facebook members voluntarily supplied ConnectU with their Facebook login information. ConnectU then used this login to comply with their requests. (*Id.* at ¶¶ 3, 4, 13.) Nothing in the statute indicates that this is insufficient "permission," and that criminal liability should attach to such activity. It could not have been the intent of the legislature to criminalize what millions of people do every day, namely, give friends their login information to a variety of websites that include personal information about the member, including web-based email, dating sites, and photograph-sharing sites, regardless of the details of the Terms of Use of any such site.

Plaintiffs conflate possible violations of Facebook.com's terms of use by Facebook's members with Defendants' allegedly unauthorized access to the website and allegedly authorized access to use information stored by members on the website under a criminal statute. Whether it violates Facebook's Terms of Service for members to share their login information to a free, public website containing information about them that they created and posted may be an interesting contractual question,[15] but Defendants' reasonable belief that they had they permission of the relevant rights-holders to access those members' Facebook profiles should be sufficient to absolve Defendants of liability under a criminal statute. At the very least, it creates a dispute of material fact as to whether Defendants' access was "unauthorized" or "without permission" as those terms are used in this criminal statute, strictly construed.

C. Plaintiffs Offer No Evidence That They Are an "Owner or Lessee"

Section 502(e)(1) places several conditions on any person or entity attempting to bring a civil action under the statute. The first gives only the "**owner or lessee** of the computer [or] computer system" the right to pursue a civil action under § 502. (Emphasis added.) Neither the term "owner" nor the term "lessee" is defined in the statute. Neither Facebook nor Zuckerberg offer any proof whatsoever that either was an "owner or lessee" of the facebook.com website when the allegedly wrongful conduct occurred, as required by the statute. Indeed, they did not even make the allegation in their Motion. It is entirely possible that another entity that Zuckerberg created, Thefacebook LLC, and/or other individuals, owned the Facebook website during the relevant period. (*See* Mosko Decl. Ex. A, Zuckerberg Dep. Trans. at p. 45:6-25, 62: 1-24, 63: 1-25, 64: 1-20.) This failure of

[15] Plaintiffs cite to this Court's decision on ConnectU's Motion to Dismiss to establish that the access was unauthorized. (Mot. at 18.) Defendants disagree with Plaintiffs' interpretation of that decision, which was not a decision on the merits of the parties' claims or defenses. *See* Section I, fn. 1, *supra*.

proof indicates that neither Facebook nor Zuckerberg has standing to assert this claim. Accordingly, summary judgment is not appropriate.

D. Plaintiffs Suffered No "Damage or Loss" as a Result of Defendants' Actions

Section 502(e)(1) also requires that the owner or lessee "suffer[] damage or loss" as a result of the defendant's actions. The statute does not define what constitutes "damage or loss" under § 502(e). In fact, Zuckerberg had a hard time articulating any damages he or Facebook suffered as a result of Defendants' alleged actions. (See Section IV.A.3, *supra* and Mosko Decl., Ex. A, Zuckerberg Dep. Trans. at p. 242: 7-18, 243: 17-25, 244: 1-25, 245: 1-25, 246: 1-19.) Whether Plaintiffs suffered damage or loss is therefore a dispute of material fact. In an attempt to rehabilitate Zuckerberg's admission of no damages and show "damage or loss," Plaintiffs rely on § 502(b)(9) and *U.S. v. Middleton*, 231 F.3d 1207 (9th Cir. 2000). (Mot. at 17.) As explained below, neither supports Plaintiffs' position.

Moreover, contrary to Plaintiffs' misleading arguments, Plaintiffs did not "engage in efforts to prevent Defendants from gaining further unauthorized access." (*Id.* at 16.) None of the "efforts" in the code analyzed by Shiflett, and as explained in Shiflett's declaration, were made **in direct response** to Defendants' alleged actions. (Williams Decl. ¶¶ 21, 22.) Indeed, all of the "efforts" in the code and in Shiflett's declaration were to bring the Facebook website in line with other, similar website security practices, not necessarily in response to Defendants' actions. (*Id.* at ¶ 22.) Accordingly, even assuming that Plaintiffs' efforts to restore their system could be considered damage or loss under § 502, none of the efforts outlined in Shiflett's declaration were in response to Defendants' alleged actions, and there is a genuine issue of material fact as to whether Plaintiffs have suffered damage or loss.

1. "Victim Expenditure" Is Not Synonymous with "Damage or Loss"

Regarding § 502(b)(9), which is the definition of "victim expenditure," this section gives no indication that it is to be applied to § 502(e). Indeed, the phrase "victim expenditure" is not present in § 502(e) and use of the term "victim" implies that it applies only to the criminal provisions of the statute, as civil litigants are not commonly referred to as "victims" and the phrase is used only in connection with § 502(d) of the statute, which details the jail sentences and other punishments to be imposed if a defendant is found guilty of a crime. To the extent that the Court believes that § 502(b)(9) sheds light on the phrase "damage or loss" found in § 502(e)(1), nothing in the definition of "victim expenditure" allows a plaintiff to pursue damages of the nature noted by Plaintiffs. Specifically, Plaintiffs claim that they spent time modifying the Facebook source code (Mot. at 16) to deal with a perceived threat and make the website more secure. These modifications do not meet the definition of "victim expenditure," which is limited to expenditures made to "**verify** that the computer system . . . was not altered, deleted, damaged, or destroyed by the access." Cal. Penal Code § 502(b)(9) (emphasis added). Whether any of the work described in Plaintiffs' Motion constitutes "verification" is at least a dispute of material fact that precludes summary judgment.

2. Additional Programming, If Any, Is Not Sufficient Damage or Loss

Plaintiffs rely exclusively on *U.S. v. Middleton*, 231 F.3d 1207 (9th Cir. 2000) to show that they suffered "damage or loss" as required by the statute. (Mot. at 17.) Specifically, in a misguided attempt to establish the necessary element of "damage or loss" under § 502(c), Plaintiffs state that "hours spent fixing computer programs to deal with a computer attack is damage." (*Id.*) *Middleton*, however, is easily distinguishable on the facts and law.

In *Middleton*, a former employee gained unauthorized access to his former employer's computer system and, among other things, "changed all the administrative passwords, altered the computer's registry, deleted the entire billing system (including programs that ran the billing software), and deleted two internal databases." 231 F.3d at 1209. In affirming the district court's jury instructions and underlying conviction, the Ninth Circuit stated that a prosecutor can establish the necessary element of 'damage or loss' by introducing evidence that the victim incurred costs to **restore** the data, program, system, or information that was damaged. *Id.* at 1213. The Ninth Circuit further agreed that the lower court's jury instructions properly indicated that the appropriate measure of damage or loss include those costs associated with resecuring the employers' computer system (i.e. making the system as secure before the defendants' actions), but not making it more secure than it was before. *Id.*[16]

The Central District of California, in a case decided after *Middleton*, faced a similar issue in *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1280 (C.D. Cal. 2001) ("The question presented by the parties is whether a plaintiff must suffer economic damages in order to bring a claim under Section 1030(g)."). After a thorough analysis of the statute, and the "suffered damage or loss" language in particular, the court stated that "it is clear . . . that 'loss' as it is used in Section 1030(g) means irreparable damage . . . [a]ny broader interpretation of the term 'loss' would render the term 'damage' superfluous." *Id.* at 1281. Ultimately, the court concluded that noneconomic damages are not recoverable by a plaintiff unless the plaintiff suffers damage as defined by the statute.[17] (*Id.* at 1281.)

Although neither *Middleton* nor *Intuit* examined the required elements of California Penal Code § 502(e), both analyzed the phrase "suffered damage or loss" in the context of a federal statute with a similar requirement. Both cases allow for the recovery of physical damage caused by a violation of the underlying statute. Importantly, both decisions interpret the "damage or loss" requirement to be limited to resecuring a computer network. The Ninth Circuit went so far as to preclude recovery for any costs associated with upgrading the security measures of a computer system in response to a violation of the federal statute. *Middleton*, 231 F.3d at 1213.

---

[16] Although the element "suffers damage or loss" has never been interpreted in the context of a § 502(c) action, California courts have interpreted the term in the context of 18 U.S.C. § 1030, a federal statute with a similar damages requirement. Both statutes prohibit the unauthorized access of a computer or computer systems and allow those who have "suffered damage or loss" as a result of the unauthorized access to bring a civil action against the alleged violator. *See* Cal. Penal Code § 502(c) and 18 U.S.C. § 1030. Specifically, § 1030(g) states that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." (Emphasis added.) Section 502(e)(1) states that "the owner or lessee of a computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief."

[17] Section 1030(e)(8) defines damage as "any impairment to the integrity or availability of data, a program, a system, or information, that (A) causes loss aggregating at least $5,000 in value during any one year period to one or more individuals . . . ." 18 U.S.C. § 1030(e)(8).

In an effort to establish damage or loss under § 502(e), Plaintiffs describe the steps allegedly taken to counter Defendants' alleged actions regarding the Facebook website. Specifically, these countermeasures included: "(1) **developing software** (using javascript) to conceal email addresses from software designed automatically to steal this information; (2) **rendering users' email addresses as images** . . . so as to require the use of optical character recognition ("OCR") software to copy email addresses . . . ; and (3) **writing code to specifically identify ConnectU's malicious "agents"** and to prevent them from accessing the site." (Mot. at 16-17 (emphases added).) In addition, Plaintiffs claim that Plaintiff Zuckerberg and Dustin Moskovitz "spent at least four days **producing the new code to counteract Defendants' efforts** to access the Facebook website." (*Id.* at 17) (emphasis added).

The alleged damage or loss suffered by Plaintiffs does not comport with the standards set forth in either *Middleton* or *Intuit*, discussed above. First, none of the "countermeasures" have been directly attributed to the alleged actions of Defendants. In other words, Plaintiffs offered no evidence that the measures they describe were taken solely in response to Defendants' activities. (Williams Decl. ¶ 21.) If Defendants' activities were not the sole cause of these additional security measures, Defendants cannot be found liable under § 502. Even if Plaintiffs establish that their measures were taken in response to Defendants' alleged actions, Plaintiffs' responses can only be considered countermeasures to Defendants' alleged actions and not the steps one would take to **resecure** the facebook.com website. All of the "damages" described by Plaintiffs above, i.e., developing new software, rendering email addresses as images, writing code to identify Defendants' malicious "agents" and producing new code to counteract Defendants' alleged efforts are nothing more than measures resulting in a new and better security system for facebook.com. These are exactly the type of measures that were not considered damages in *Middleton* or *Intuit*, and should not be considered "damage or loss" within the meaning of § 502(e).

It is a dispute of material fact whether Facebook or Zuckerberg incurred any damage or loss cognizable under § 502(e), and summary judgment is not appropriate.

E. The Data Obtained by ConnectU is not Private

Cal. Penal Code § 502(a) notes that one of the purposes of the statute is for the "protection of the privacy of individuals. . . ." Because Plaintiffs have not established that any of the information allegedly obtained by ConnectU was "private" information, summary judgment is not appropriate.[18] Although ConnectU admits that it found email addresses on the Facebook members' profile pages, ConnectU disputes that this information is private and within the scope of Cal. Penal Code § 502. ConnectU's actions, do not, therefore, fall within the purpose of the statute, strictly construed, and summary judgment must be denied.

Facebook.com allows each member to create a profile which includes a variety of information, depending on what a user posts. (Second Am. Compl. ¶ 10.) This profile often includes contact information, including cell phone numbers, email addresses, home addresses, photographs, and other identifying information. (*Id.*) The profiles are accessible by other members of facebook.com, who are not under any obligation to maintain this information in confidence. Indeed, the purpose of the profile is to have other's view and comment on it. When personal information is put in the public domain, even in a limited way, it loses any privacy interest. *Nader v. General Motors Corp.*, 255 N.E. 2d 765 (NY 1970). For example, in *Wilson v. Harvey*, 842 N.E.2d 83 (Ohio Ct. App. 2005), some students posted fliers around campus which featured a classmate's email address and phone number. The Ohio court held that this was not an invasion of privacy because the information was accessible to all students and faculty on the university's website. *Id.* at 91. Importantly, the university website was also a form of limited disclosure (available to students and staff) discussed by this Court in its Order on the Motion to Dismiss. The Ohio court nonetheless concluded that the information was not sufficiently concealed or veiled to support a privacy claim. *Id. See also, Ossur Holdings, Inc. v. Bellacure, Inc.* No. 05-1552, 2005 WL 3434440, at *6 (W.D. Wash. Dec. 14, 2005) (denying a preliminary injunction for breach of a confidentiality agreement because the names and email addresses allegedly disclosed in breach of agreement were generally known to the public).

---

[18] Facebook argues that the Court has already settled this issue. (Mot. at 17, fn. 9.) As detailed in Section I. fn. 1, *supra*, the Court was considering a Motion to Dismiss not a motion for summary judgment.

Whether the information obtained by ConnectU was private pursuant to § 502(a) is a dispute of material fact, precluding summary judgment.

VI. PLAINTIFFS' UNCLEAN HANDS PRECLUDE SUMMARY JUDGMENT

Plaintiffs cannot succeed on summary judgment because there is a genuine issue of material fact as to whether Defendants' unclean hands affirmative defense bars some or all of the relief Plaintiffs seek in the Second Amended Complaint. (*See* Defs.' Second Am. Answer ¶ 84.)

A. Zuckerberg's Attempts to Hack ConnectU's Servers Constitute Unclean Hands

Plaintiffs have engaged in wrongful conduct, which should bar recovery or limit the remedies available to them in this case. The Declaration of Hunter Jones shows that [redacted]

As one California Appellate Court has explained, "The doctrine [of unclean hands] demands that a plaintiff act fairly in the matter for which he seeks a remedy . . . regardless of the merits of his claim." *Kendall-Jackson Winery, Ltd. v. Superior Court*, 76 Cal. App. 4th 970, 978-79 (citations omitted). Whether the doctrine of unclean hands applies is a question of fact. *See CrossTalk Prods., Inc. v. Jacobson*, 65 Cal. App. 4th 631, 639. In deciding whether a claim is barred by a plaintiff's unclean hands, California courts consider three factors: (1) analogous case law; (2) the nature of the misconduct; and (3) the relationship of the misconduct to the claimed injuries. *Blain v. Doctor's Co.*, 222 Cal. App. 3d 1048, 1060.

In this case, analogous case law supports application of the unclean hands doctrine to Plaintiffs' claim under California Penal Code § 502. In *Unilogic Inc. v. Burroughs Corp.*, 10 Cal. App. 4th 612, the parties agreed to cooperate in a joint enterprise to develop computer prototypes. Burroughs licensed computer code to Unilogic, which was to be returned to Burroughs should the joint enterprise end. *Id.* at 616. The joint enterprise was a failure, and the parties initiated a lawsuit involving multiple claims and counterclaims. *Id.* at 616-17. Following trial, Unilogic's conversion claim went to the jury. It was partially based on Unilogic's allegation that a Burroughs employee had "spirited proprietary information away from Unilogic" at the direction of Burroughs. *Id.* at 618.

The jury unanimously found in Unilogic's favor on the conversion claim but awarded no damages based on a finding in Burroughs's favor on its unclean hands defense. *Id.* at 617. The California appeals court upheld the application of the unclean hands defense and the jury's findings. *Id.* at 623. The defendant's misconduct in *Unilogic* is analogous to Facebook's allegations of "unauthorized access" under California Penal Code § 502.[19] *See also Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 40 (Cal. 1990) (unclean hands defense could bar a violation of a state constitutional right of privacy); *Fuddruckers, Inc. v. Doc's B.R. Others, Inc.*, 826 F.2d 837, 847 (9th Cir. 1987) (applying unclean hands to Lanham Act violations).

The nature of the misconduct shows Zuckerberg's clear intention to infiltrate ConnectU's servers wrongfully. Bad intent is the essence of the unclean hands misconduct. *Wells Fargo & Co. v. Stagecoach Props., Inc.*, 685 F.2d 302, 308 (9th Cir. 1982). The misconduct need not be a crime or an actionable tort; any conduct that violates conscience, or good faith, or other equitable standards of conduct is sufficient cause to invoke the doctrine. *DeRosa v. Transam. Title Ins. Co.*, 213 Cal. App. 3d 1390, 1395-96 (1989) (citations omitted). Finally, Defendants can clearly show the necessary connection between Plaintiffs' misconduct and the issues of this case. *See Kendall-Jackson Winery*, 76 Cal. App. 4th at 985 ("[a]ny evidence of a plaintiff's unclean hands in relation to the transaction before the court or which affects the equitable relations between the litigants in the matter before the court should be available to enable the court to effect a fair result in the litigation.").

B. Unclean Hands Defense Creates a Genuine Issue of Material Fact

Mark Zuckerberg's [redacted] activities raise a genuine issue of material fact as to whether Defendants' unclean hands defense applies in this case. Zuckerberg is Facebook's founder, CEO, and chairman of the board, and therefore his unclean hands can be attributed to Facebook as well. *See* Mosko Decl., Ex. A, Zuckerberg Dep. Trans.at p.10: 9-19, 35: 2-17.) Summary judgment in favor of Plaintiffs is therefore inappropriate. "When plaintiff is the moving party [for summary judgment on liability], plaintiff's burden of proof is: (1) to demonstrate affirmatively (by admissible evidence) that there is no genuine issue of material fact as to each element of its claim for relief, entitling it to judgment as a matter of law; and (2) **to demonstrate the lack of any genuine issue of material fact as to affirmative defenses asserted by the defendant**." *Kaap Indus. v. Burns & McDonnell Eng'g Co. Inc.*, Case No. CV F 06-0417, 2007 U.S. Dist. LEXIS 66064, at *7-8 (E.D. Cal. Aug. 27, 2007) (emphasis added). Unclean hands is a fact-intensive inquiry not amendable to disposition on summary judgment. *See Mattco Forge, Inc. v. Arthur Young & Co.*, 5 Cal. App. 4th 392, 407-08 ("As a general rule, application of the unclean hands doctrine remains primarily a question of fact . . . . As such it is not properly determined . . . on a summary judgment motion.") (citations omitted). The Ninth Circuit has noted that the unclean hands defense primarily involves questions of fact reviewed for clear error. *See, e.g., L.A. News Serv. v. Tullo*, 973 F.2d 791, 799 (9th Cir. 1992); *Dollar Sys., Inc. v. Avcar Leasing Sys., Inc.*, 890 F.2d 165, 173 (9th Cir. 1989).

---

[19] The analogy need not be perfect. Indeed, Unilogic argued that the equitable defense of unclean hands may not be asserted as an affirmative defense to a legal action for conversion. The court found no authority on point, but concluded that Unilogic had "not provided [the court] with any reason, based on policy or otherwise, for holding that the unclean hands defense is never available in a legal action for conversion," and declined to so hold. *Unilogic*, 10 Cal. App. 4th at 620.

C. Unclean Hands Is Available as a Defense to All of Plaintiffs' Claims

Facebook argued in its opposition to Defendants' Civil L.R. 6-3 Motion that "unclean hands is not an available defense to a statutory violation," citing *Lass v. Eliassen*, 94 Cal. App. 175, 179, and *Timberline v. Jaisinghani*, 54 Cal. App. 4th 1361, 1368. Those cases involved comprehensive statutory schemes governing probate and corporations respectively. There is no general bar to using unclean hands to defend against a civil action that is established by statute. Moreover, Plaintiffs' prayer for relief asks for injunctive and other equitable relief, both generally and under "California Penal Code § 502(c) et seq." (*See* Pls.' Second Am. Compl. ¶¶ 9, 11-13, 15.) California law explicitly allows unclean hands as a defense against both legal and equitable claims. *See Fibreboard Paper Prods. Corp. v. E. Bay Union of Machinists*, 227 Cal. App. 2d 675, 728 ("We are satisfied that the equitable defense of unclean hands is available in this state as a defense to a legal action."); *Adler v. Fed. Republic of Nig.*, 219 F.3d 869, 877 (9th Cir. 2000) (citing *Jacobs v. Universal Dev. Corp.*, 53 Cal. App. 4th 692, 699 (1997)) ("In California, the unclean hands doctrine applies not only to equitable claims, but also to legal ones."). Further, courts in the Ninth Circuit have applied unclean hands to legal actions. *See Metro Publ'g v. San Jose Mercury News*, 861 F. Supp. 870

(N.D. Cal. 1994) (stating that "[s]everal courts have applied the equitable doctrine of unclean hands to bar actions for legal damages." Further, at least one Circuit Court of Appeals has noted that the merging of law and equity may have rendered the traditional application of unclean hands only to equitable claims obsolete. *Byron v. Clay*, 867 F.2d 1049, 1052 (7th Cir. 1989) (citations omitted).

Accordingly, the equitable defense of unclean hands is available to defeat both the CAN-SPAM and the California Penal Code § 502 claims, and precludes summary judgment.

VII. UNDER FED. R. CIV. P. 56(f), SUMMARY JUDGMENT IS PREMATURE PENDING FURTHER DISCOVERY

This Court should deny Plaintiffs' motion based on the disputes of material fact detailed above. To the extent the Court is not persuaded by Defendants' positions, Defendants respectfully remind the Court that discovery necessary to defend against these claims is incomplete, and as reflected in their Fed. R. Civ. P. 56(f) motion filed January 10, 2008. (Dkt. 259.)

Importantly, Defendants need additional discovery to take Facebook's Fed. R. Civ. P. 30(b)(6) deposition regarding the design of Facebook's servers used to operate its website, including information regarding bandwidth capabilities and network functionality. This information is relevant to demonstrate that Plaintiffs were not adversely affected, as that term is used in the CAN-SPAM Act, by any of Defendants' alleged conduct because Plaintiffs' servers were not forced to suffer increased bandwidth or network functionality difficulties as a result of any of Defendants' alleged conduct in violation of CAN-SPAM. On January 17, 2008, immediately after the case management conference, Defendants asked Plaintiffs to make a 30(b)(6) witness available for deposition as soon as possible. Plaintiffs initially refused, then stalled by falsely claiming that they did not understand the purpose of the deposition. Finally, on January 30, 2008, Plaintiffs offered to make the witness available *after* the date on which Defendants' opposition to Plaintiffs' Motion was due. (Mosko Decl., Ex. B). Defendants should be able to complete their discovery and provide the results of it before this Court rules on Plaintiffs' motion.

VIII. CONCLUSION

For the reasons stated above, the Court should deny Plaintiffs' Motion for Partial Summary Judgment.

Dated: February 6, 2008

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

By: /s/
Scott R. Mosko
Attorneys for Defendants ConnectU LLC, Pacific Northwest Software, Inc., Winston Williams, and Wayne Chang